AO 106 (Rev. 01/09) Application for a Search Warrant

United States District Court

for the
Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)
Email account: **SCOTTSANSTROM@YAHOO.COM**

THAT IS STORED AT PREMISES OWNED, MAINTAINED, CONTROLLED, OR OPERATED BY OATH HOLDINGS, INC., AN E-MAIL PROVIDER HEADQUARTERED AT 701 FIRST AVENUE, SUNNYVALE, CALIFORNIA 94089

Case No. 19-MJ-1040

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

E-mail account SCOTTSANSTROM@YAHOO.COM, stored at premises owned, maintained, controlled, or operated by Oath Holdings, Inc., an email provider headquartered at 701 First Ave, Sunnyvale, California 94089. See **Attachment A** which is incorporated herein.

there is now concealed: *(identify the person or describe the property to be seized)*:

See **Attachment B**, for Particular Items to Be Searched for and Seized attached herein and incorporated by reference.

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. §2251(a), 2252A(a)(2), 2252A(a)(5)(B) and 2252A(b)(1) and (2).

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☒ Delayed notice of 60 days (give exact ending date if more than 30 days: May 28, 2019) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature
TASK FORCE OFFICER MICHAEL HOCKWATER
FEDERAL BUREAU OF INVESTIGATION
Printed name and title

Sworn to before me and signed in my presence.

Date: March 29, 2019

Judge's signature
HONORABLE JEREMIAH J. MCCARTHY
UNITED STATES MAGISTRATE JUDGE
Printed name and Title

City and state: Buffalo, New York

ATTACHMENT A
Property to Be Searched

Yahoo! email account **scottsanstrom@yahoo.**com that is stored at premises owned, maintained, controlled, or operated by Oath Holdings Inc., an e-mail provider headquartered at 701 First Ave, Sunnyvale, California 94089

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Oath Holdings Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of **Oath Holdings Inc.**, **Oath Holdings Inc.** is required to disclose the following information to the government for the account or identifier listed in Attachment A:

a. The contents of all e-mails stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. The contents of all instant messages stored in the account, including copies of messages sent to and from the account, draft messages, the source and destination addresses associated with each message, the date and time at which a message was sent/received, and the size and length of each message;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between Oath Holdings Inc., and any person regarding the account, including contacts with support services and records of actions taken.

II. Information/Items to be seized by the government

All records, data and information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2251(a) - Production and Attempted Production of Child Pornography, § 2252A(a)(2)(A) and § 2252A(b)(1) - Receipt and Attempted Receipt of Child Pornography, and § 2252A(a)(5)(B) and § 2252A(b)(2) - Possession and Attempted Possession of Child Pornography, including, for the account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence of the possession, receipt, distribution or production or of images depicting minors engaging in sexually explicit conduct, including attempts;

b. Any and all items and communications, including attachments, and images or videos, related to the possession, receipt or production, including attempts, of images depicting minors engaging in sexually explicit conduct and associated data, including but not limited to ip addresses, any the source and destination addresses associated with each, and associated records of the date and time; or

c. Any records or data or other information relating to who created or used the email account or identifier listed in Attachment A, including records which help to identify the user and the user's whereabouts.

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Michael Hockwater, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Police Detective with the Town of Cheektowaga, New York Police Department. I have been a Police Officer since August of 1989. I am currently assigned as a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), Buffalo Field Office, Child Exploitation Task Force (CETF), Innocent Images National Initiative, which targets individuals involved in the on line sexual exploitation of children. I have been a TFO since June 14, 2010. As part of these duties, I have become involved in the investigation of suspected violations of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422, and 2423. I have also participated in various FBI mandated and volunteer training for the investigation and enforcement of federal child pornography laws in which computers are used as the means for receiving, transmitting, and storing child pornography.

2. I make this affidavit in support of an application for a search warrant for information associated with a certain Yahoo! email account that is stored at premises owned, maintained, controlled, or operated by Oath Holdings Inc., an e-mail provider headquartered at 701 First Ave, Sunnyvale, California 94089. The information to be searched is described in the following paragraphs and in Attachment A.

3. This affidavit is made in support of a search warrant, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, and 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to search the following property, where I believe evidence of violations of 18 U.S.C. § 2251(a) (production and attempted production of child pornography), 18 U.S.C. § 2252A(a)(2) and § 2252A(b)(1), (receipt and attempted receipt of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) and § 2252A(b)(2) (possession and attempted possession of child pornography) (collectively, the "SUBJECT OFFENSES") will be located in Yahoo email account **SCOTTSANSTROM@YAHOO.COM** (hereinafter "TARGET ACCOUNT"). The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2251(a), § 2252A(a)(2) and §2252A(b)(1) and § 2252A(a)(5)(B) and §2252A(b)(2) have been committed by a person using the TARGET ACCOUNT and/or others. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

II. COMPUTERS AND ENTICEMENT

5. Computers and computer technology have revolutionized the way in which

individuals interact with minors for the purposes of engaging in sexual activities. Through the use of computers and the internet, individuals have to ability to easily seek out, solicit, entice, coerce, and/or coordinate meetings with minors for the purpose of engaging in sexual activity. Individuals typically use social networking sites, online community sites, cellular telephones, and other internet browsers/search engines to facilitate these activities. The goal is to establish a relationship over the internet that can eventually lead to a face-to-face meeting for the purposes of engaging in sexual activities with the minor(s).

6. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider (ISP) that connects to the Internet. The ISP assigns each user an Internet Protocol (IP) Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP

addresses may also be static, if an ISP assigns a user's computer a particular IP address that is used each time that computer accesses the Internet. The ISP may log the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

7. Yahoo! is a web services provider that, among other functions, provides users with e-mail services, and allows users to communicate via the Internet with other Internet users. Yahoo.com is owned and operated by Verizon Media operating under the entity known as Oath Holdings Inc.

8. In order to use the email features of Yahoo!, an individual must register with Yahoo! by establishing a unique screen name, user profile, and password. During registration or at any time after registration, an individual may add other personal information, such as their name, address, telephone number, interests, etc., to their user profile. After registration is complete with Yahoo!, an email account will be established and accessible for the individual with the email address [unique screen name]@yahoo.com.

III. PROBABLE CAUSE

9. On February 27, 2019, I was contacted by the Town of Cheektowaga Police Department who was investigating an incident wherein a 10 year old minor female (hereinafter VIC1) had been communicating with an unidentified person (SUBJECT1) who was utilizing the TARGET ACCOUNT. VIC1 was using an Apple email account with

identifiers known to me. SUBJECT1 sent VIC1 naked pictures of himself and requested that VIC1 send him pictures showing her naked body. On February 27, 2019, I spoke with the father of VIC1 who authorized a search of her iPad.

10. On March 1, 2019, I searched the iPad belonging to VIC1 and found several emails between VIC1 and the TARGET ACCOUNT. The email communications between VIC1 and the TARGET ACCOUNT began on February 21, 2019 and ended on February 25, 2019. On February 21, 2019 at 2:24 PM EST, VIC1 sent a picture of her genital area to the TARGET ACCOUNT. On the same day at 3:19 PM EST, VIC1 sent a naked picture of her whole body to the TARGET ACCOUNT. On February 21, 2019 at 4:35 PM EST, the user of the TARGET ACCOUNT sent VIC1 an email stating "Good I miss you, Can I still call you babe". On the same day at 4:38 PM EST, the user of the TARGET ACCOUNT sent VIC1 a picture of his genitals. On the same day at 4:42 PM EST, the user of the TARGET ACCOUNT sent VIC1 and email stating, "Send me sexy video of you". Four minutes later, the user of the TARGET ACCOUNT sent VIC1 and email stating, "send me rub pussy".

11. On March 5, 2019, VIC1 was forensically interviewed at the Child Advocacy Center in Buffalo, New York. VIC1 stated that she had first met SUBJECT1 at the end of 2018 before Christmas on a mobile application called "MLB9INNINGS"and soon after their communications switched to email. VIC1 posted on her "MLB9INNINGS" account that she was 10 years old. SUBJECT1 used email address SCOTTSANSTROM@YAHOO.COM. VIC1 stated that SUBJECT1 initially told her that he was 11 years old and asked her to send

him naked pictures of herself. At the request of SUBJECT1, VIC1 sent several pictures of herself displaying her genitals to the TARGET ACCOUNT. SUBJECT1 also sent VIC1 pictures of his genitals and his face at which time VIC1 realized that SUBJECT1 was older estimating that he was in his thirties. SUBJECT1 told VIC1 that he wanted to drive to her house to meet her in person.

12. On or about March 28, 2019, I sent an Administrative Subpoena to Oath Holdings, requesting subscriber information and ip logs for the TARGET ACCOUNT. On March 13, 2019, I reviewed the results of that subpoena and discovered that the subscriber was Scott Sanstrom, 610 E. Kerr Ave. Apt. 105, Urbana, Illinois 61802, telephone number (217) 344-8325. The subpoena return also provided ip connection logs. The most recent login was on February 26, 2019 at 7:20:42 PM (GMT). The ip address used at that date and time was 2601:240:8201:9e0:3d8f:b3e1:f561:4a48. A subpoena for that ip address identified the subscriber as Scott Sanstrom, 610 E. Kerr Ave. Apt. 105, Urbana, IL 61802, telephone number (217) 344-8325.

IV. TECHNICAL BACKGROUND

13. In my training and experience, I have learned that YAHOO!, Inc. provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. YAHOO! Inc. allows subscribers to obtain e-mail accounts at the domain name yahoo.com, like the e-mail accounts listed in Attachment A. Subscribers obtain an account by registering with YAHOO, Inc. During the registration process, YAHOO!, Inc. asks subscribers to

provide basic personal information. Therefore, the computers of YAHOO!, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for YAHOO!, Inc. subscribers) and information concerning subscribers and their use of YAHOO!, Inc. services, such as account access information, e-mail transaction information, and account application information.

14. In general, an e-mail that is sent to a YAHOO!, Inc. subscriber is stored in the subscriber's "mail box" on YAHOO!, Inc. servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on YAHOO!, Inc. servers indefinitely.

15. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to YAHOO!, Inc.'s servers, and then transmitted to its end destination. YAHOO!, Inc. often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the YAHOO!, Inc. server, the e-mail can remain on the system indefinitely.

16. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by YAHOO!, Inc. but may not include all of these categories of data.

17. A YAHOO!, Inc. subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by YAHOO! Inc., which allows users to search for videos on the internet.

18. Subscribers to YAHOO!, Inc. might not store on their home computers copies of the e-mails stored in their YAHOO!, Inc. account. This is particularly true when they access their YAHOO!, Inc. account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

19. In general, web service providers like YAHOO!, Inc. ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

20. Web service providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via YAHOO!, Inc.'s website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address

("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

21. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

22. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

V. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

23. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Oath Holdings Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B,

government-authorized persons will review that information to locate the items described in Section II of Attachment B.

VI. CONCLUSION

24. Based upon the above information, I believe that probable cause exists to believe there has been a violation of Title 18, United States Code, Sections 2251(a), 2252A(a)(2) and § 2252A(b)(1), and 2252A(a)(5)(B) and § 2252A(b)(2) and that there is probable cause to believe that in the TARGET ACCOUNT, there is located the items set out in **Attachment A.**

25. Based upon the foregoing, I request that the Court issue the proposed search warrant for the TARGET ACCOUNT.

26. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

27. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

VI. REQUEST FOR SEALING

28. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed for 60 days or until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Michael Hockwater, Task Force Officer
Federal Bureau of Investigation

Sworn and subscribed to before me
this 29th day of March 2019.

HONORABLE JEREMIAH J. MCCARTHY
United States Magistrate Judge